An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture

Amelie Gyrard, Christian Bonnet, Karima Boudaoud

An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture

Amelie Gyrard, Christian Bonnet
Mobile Communication
Eurecom
Biot, France
Email: {gyrard,bonnet}@eurecom.fr

Karima Boudaoud
Rainbow team
Laboratoire I3S-CNRS/UNSA
Biot, France
Email: karima@polytech.unice.fr

***Abstract*—Securing the Internet of Things, more precisely, the ETSI Machine to Machine (M2M) architecture is a difficult task, since there is a need to secure heterogeneous wireless communications (cellular, wireless, wired), devices (sensor or mobile phone) and applications (programming language, framework, database). In this article, we present the state of the art concerning the security ontologies in various domains (Web, MANET, 2G/GSM, 3G/UMTS, 4G/LTE, Wi-Fi, Intrusion Detection System). Since, most of the existing security ontologies are not published online or do not follow semantic web best practices, we have designed the STAC (Security Toolbox: Attack & Countermeasure) ontology-based security knowledge respecting the semantic web guidelines. The STAC ontology, dataset and application have been designed to help software developers or designers to choose security mechanisms fitting their needs to secure Internet of Things (IoT) applications. STAC is published online (http://sensormeasurement.appspot.com/?p=stac).**

***Keywords*-Security ontologies; Semantic Web; OWL; Internet of Things; ETSI Machine to Machine (M2M); Semantic Web of Things; 2G/GSM; 3G/UMTS; 4G/LTE; Wi-Fi; WLAN; Security Property; Cryptography; Security Protocol; Security Mechanism; Sensor Networks**

I. Introduction

On the one hand, Internet of things (IoT) combines and connects numerous things to the web such as sensors and mobile phones. IoT is a broader concept than Machine to Machine which means that machines can communicate with each other without human intervention using the network. The ETSI M2M architecture [4] is an European standard composed of: (1) the M2M area networks with M2M devices (sensor, embedded sensor or mobile phone) and M2M network communications, (2) the M2M gateways which store sensed M2M data, and (3) the M2M applications which handle M2M data. Securing the ETSI M2M architecture is a difficult task, since we have to secure heterogeneous wireless communications (cellular, wireless, wired), devices (sensor or mobile phone) and applications (programming language, framework, database).

On the other hand, we found more 24 ontology-based work related to sensor networks, mobile phones, cellular networks, IDS and cryptography. We propose to exploit these security ontologies to build a common semantic-based security knowledge to help software designers to secure the ETSI M2M architecture. Semantic web technologies are more and more used to structure the data on the Web to latter reason about them. Basic languages RDF, RDFS and OWL are mainly used to describe triplets, for example the jamming attack is a attack will be written as following `Jamming rdf:type Attack`. Such languages enable to describe the notion of hierarchy and enables to define new concepts to describe your own ontology. An ontology is a vocabulary to define main concepts and relationships between them in a specific domain. At the beginning of this work, only five ontologies were published online and did not follow the semantic web guidelines. For these reasons, we build the STAC (Security Toolbox: Attack & Countermeasure) ontology-based security knowledge and semantic web guidelines are complied with. We extend our previous work the STAC ontology [11] to build the STAC application used to help software designers or developers to secure the ETSI M2M architecture. The goal of this work is not to propose a protocol for securing IoT but to build a security knowledge base (ontology, dataset, rule) to help designers to secure their M2M applications.

To the best of our knowledge, we are the first work proposing an ontology-based approach to help software designers to secure the ETSI M2M architecture. Further, there is no concrete security solutions in the OneM2M international standard technical specification to help to secure an Internet of Things architecture.

In this article, we firstly present the state of the art concerning the security ontologies in various domains such as sensors, mobile phones, web, cryptography, 2G, 3G, 4G, Wi-Fi and IDS. We explained in section III the limitations of existing security ontologies. We present in section IV our contribution, the STAC (Security Toolbox: Attack & Countermeasure) security knowledge, a hub to combine existing security ontologies according to the semantic web best practices, more precisely, the STAC ontology, the dataset, the prototype implementation and the evaluation. Finally, we conclude the article.

II. Exploiting existing security ontologies

In this section, we present the security ontologies related to M2M devices, M2M network communications, M2M applications and M2M data.

A. Secure M2M devices

In this section, we present the security ontologies related to M2M devices, more precisely, sensors, embedded sensors or mobile phones.

1) Security Ontologies for Sensor Networks: We found only two ontologies defining the security concepts for Wireless Sensor Networks. Znaidi et al. [29] propose an ontology which defines only the classification of attacks according to the OSI model. They describe neither well-known attacks specific to the transport layer such as desynchronisation, DoS and flooding nor security mechanisms, protocols and key management specific to sensor networks. Kenfack et al. [14] define intrusions in wireless sensor networks. They classify vulnerabilities such as shared wireless medium, lack of infrastructure and easy physical accessibility by the intruders. They describe WSNs components (e.g., battery, sensor, radio). Firstly, none of these ontologies mention sensor security mechanisms and security properties. Secondly, these ontologies are not published online.

2) Security Ontologies for Mobile Phones: Beji et al. [3] design a security ontology for mobile applications divided in three sub-ontologies: (1) The Asset-Vulnerability-Threat Ontology (AVTO) to classify the vulnerabilities into three main classes: physical, software and those related to communications, (2) the Mobile Profile Ontology (MPO) and (3) the Defense Mechanism Ontology (DMO) which describes main security and cryptographic mechanisms such as digital signature, locking mechanism, encryption, key management, PKI, access control methods, algorithm and those specific to the mobile field (SIM locking). Vincent et al. [27] design an ontology-based firewall to ensure privacy protection for smartphones. They propose two ontologies: the former to represent the Semantic Web Rule Language (SWRL)[1] privacy policies, inspired by the SOUPA framework, and the latter the digital identity on smartphones using well-known ontologies FOAF[2] and VCard[3]. None of these ontologies are published online. The ontology [1] covers the domain of security in the field of mobile applications.

B. Secure M2M network communications

Several security ontologies have been found related to network communication, more precisely, cellular networks (2G, 3G, 4G) and Wi-Fi. They mainly describe security mechanisms in the physical and link OSI model layer.

[1]http://www.w3.org/Submission/SWRL/

[2]http://xmlns.com/foaf/spec/

[3]http://www.w3.org/TR/vcard-rdf/

1) Security Ontologies for Cellular Networks: Neji et al. define an ontology describing the architecture of cellular networks and the associated security mechanisms: Long Term Evolution (LTE)/4G [17], Universal Mobile Telecommunications System (UMTS)/3G [18] and Global System for Mobile Communication (GSM)/2G [19]. Alazeib et al. [2] develop an ontology for generic wireless authentication to describe GSM, UMTS and wireless Local Area Network (WLAN) network architecture, more precisely the Wi-Fi technlogy. Authentication mechanisms applied to these technologies are also presented.

2) Security Ontologies for Intrusion Detection Systems: Joshi, Undercoffer et al. [13] [25] design the Intrusion Detection System ontology with classes such as Vulnerability, Product, Attack properties and Weakness. This ontology is used to convert the National Vulnerability database (NVD) into RDF. They are compliant with Linked Data principle but not Linked Open Vocabularies principles. Tsoumas et al. [24] define security mechanisms such as firewall, antivirus and network protocols. Frye et al. [9] design the attach ontology to identify complex network attacks. Salahi et al. [22] design an ontology to predict networks attacks.

C. Secure M2M applications and M2M data

We present security ontologies describing cryptographic concepts and usual security mechanisms.

1) General Security Ontologies: Souag et al. [23] review numerous security ontologies and underline that are not published online but do not explain that most of the existing works do not follow the semantic web best practices. Kim et al. [15] create seven ontologies. The main security ontology describes security concepts such as security objectives (e.g. authentication) and network security protocols (e.g., IPSec, SSL). Another ontology describes symmetric and asymmetric algorithms, hash algorithms, key exchange algorithms and digital signatures. Herzog et al. [12] implement four ontologies defining several concepts such as assets, threats, vulnerabilities and security mechanisms. They propose some security mechanisms such as asymmetric and symmetric algorithms that are classified into block cipher or stream cipher. They propose also some secure network communication protocols such as SSL, SSH, VPN, security goals (authentication, integrity, confidentiality) and access control model (RBAC, MAC, DAC). Denker [6] [5] create two ontologies called 'security mechanisms' and 'credential'. They propose the notion of security notations to represent security properties such as authentication or confidentiality. They also define different authentication methods: certificate-based, password-based, biometrics (fingerprints, voice) and physical components (e.g., card). MASO [16] is an ontology written in French and defines symmetric/asymmetric algorithms, hash function, security goals and security mechanisms such as firewall and antivirus. Vorobiev et al. [28] define several ontologies: (1) Security Attack Ontology (SAO), (2) Security

Defence Ontology (SDO), (3) Security Asset-Vulnerability Ontology (SAVO), (4) Security Algorithm-Standard Ontology (SASO), and (5) Security Function Ontology (SFO). Evesti et al. [8] design an ontology de describe and check the age or structure of the password and the authentication level.

2) Security Ontologies for Web Applications: Fenz et al. [7] propose the AURUM framework, an ontology-based security knowledge. They do not classify security mechanisms and attacks according to the technologies. Razzaq et al. [21] classify web application attacks such as cookie poisoning, SQL injection, Cross Site Scripting (XSS) and proposed SWRL rules. Huang et al. [**?**] design an ontology-based malware bahavioral analysis called Taiwan Malware Analysis Net (TWMAN). They define the malware ontology with concepts such as trojan, backdoor, worm.

III. Limitations of The Security Ontologies

We explain that most of the existing security ontologies cannot be reused since they are not published online or do not follow the semantic web best practices.

A. Lack of unify terms

The main drawback of these ontologies is that they use different names for the same concepts which can confuse a software developer which is not expert in security. For example, we found several terms `Goal`, `SecurityNotation`, `SecurityObjective` in these ontologies for defining the same concept, that we call `SecurityProperty` to represent `Confidentiality`, `Integrity`, `Authentication`, etc. This is the case for numerous concepts: `AsymmetricAlgorithm/PublicKeyAlgorithm`, `HashFunction/HashAlgorithm`, etc.

B. Incomplete Security Knowledge

Most of these ontologies are domain specific, since they are focused on sensor networks, IDS, etc. To design a tool to help software designers to choose security mechanisms to secure IoT applications, we need to gather all of these security knowledge bases. Existing security ontologies are incomplete, they do not:

- Classify both threats and security mechanisms according to the technologies (Sensor, Cellular, Wireless, Web, Machine-to-Machine, etc.)
- Classify attacks and security mechanisms according to the OSI model.
- Indicate security mechanisms prevent threats.
- Describe strengths and weaknesses of security mechanisms. The developer needs more information to help him to choose the right security mechanisms. For example, WEP, WPA1 and WPA2 are several security mechanisms to secure the Wi-Fi communication. The developer wants to know that WPA2 replaces previous security mechanisms: WEP and WPA1 because they are deprecated.
- Explain that security mechanisms are composed of other security mechanisms, i.e., the Virtual Private Network (VPN) is a security mechanism which uses the IPSec protocol and the Internet Key Exchange (IKE) key management.
- Specify the relationships between security mechanisms and security properties, i.e., the Secure Shell (SSH) satisfies the authentication, integrity and confidentiality properties.

C. Lack of Semantic Web Best Practices

Unfortunately, semantic experts are not aware of semantic web best practices and semantic tools to reference their ontologies or datasets. Most of the existing security ontologies:

- Are not published online.
- Are not linked to existing security ontologies for similar concepts.
- Do not differentiate the ontology and the dataset
- Are not referenced on the Linked Open Vocabularies[4] catalogue.

D. Summary

The presented ontologies have been created without considering other existing ontologies and cannot be reused since they are not published online or do not follow the semantic web best practices. To facilitate the developer tasks, we create our own ontology, called STAC (Security ToolBox: Attacks & Countermeasure) to unify the terms, to gather security concepts in a same knowledge base and to publish online the security knowledge according to the semantic web best practices.

IV. STAC (Security Toolbox: Attack & Countermeasure): the Proposed Semantic-Based Security Approach

We have been inspired by the exiting security ontologies to design an ontology-based security knowledge called STAC (Security Toolbox: Attack & Countermeasure) [11] respecting the semantic web guidelines. This security knowledge is a hub to link existing security ontologies [1] [15] [16] published online and has been validated by the semantic web community. The STAC knowledge base enables to link security ontologies together as depicted in the Figure 1.

The purpose of the STAC ontology and dataset is to help developers and project managers to secure the IoT-based applications to ensure 'security by design' from the beginning of the project.

[4]http://lov.okfn.org/dataset/lov/

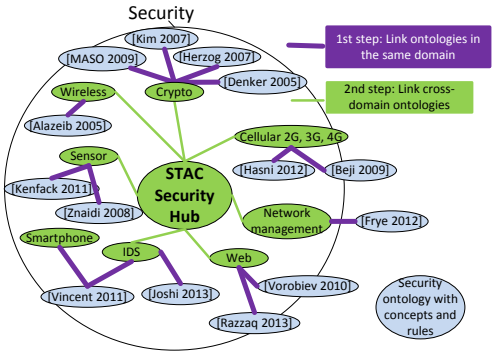

Figure 1. The STAC knowledge base

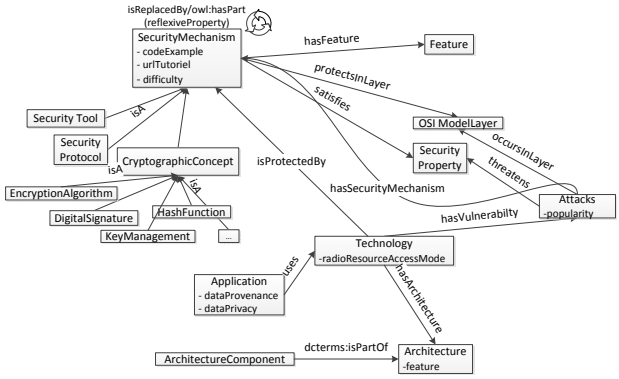

Figure 2. The top level part of the STAC ontology

A. Semantic Web Guidelines

We share the lessons learned and remind in this section the semantic web best practices that we acquired through this work for the next designers of security ontologies.

Security experts should share their ontologies, datasets and rules on the semantic web tools.

- Reference domain ontologies on the LOV catalogue[5] [26] and the semantic search engines such as Watson and Swoogle.
- Reference domain datasets on the DataHub project[6] and on semantic search engines such as Sindice[7].
- Reference domain rules on the Linked Open Rules [8] which is still a work in progress.

1) Semantic guidelines:

- To have your ontology referenced on LOV:
  - Share online your ontology
  - The name of the ontology (namespace) and the location of the ontology are the same (URI deferencable).
  - Add the metadata descriptions proposed by LOV [26] (rights, authors, licenses)
  - Add the properties `rdfs:label` and `rdfs:comment` at least in english and in another language if needed.
  - Add the property `owl:equivalentClass` with the common class already described and referenced by LOV.
  - If you encounter errors when submitting on LOV, check you ontology on Vapour[9] and TripleChecker[10]
- Follow the semantic web best practices to design your ontology [20] and the OOPS project[11] to detect common ontology pitfalls.
- Use the Linked Data principles[12] to create a well-designed RDF dataset.

We describe all semantic bad practices encountered and the related guidelines to remedy them in a draft document [10] for the OneM2M international standard.

B. STAC ontology & dataset

The STAC ontology describes main security and cryptographic concepts in various security domains such as sensor, cellular, wireless, web, IDS and network management. The main goal is to suggest the best security mechanism to design a secure application. To perform this task, we define the STAC ontology specifying relationships between `Attack`, `SecurityMechanism`, `Technology`, `SecurityProperty` and the `OSIModel` (Figure 2). In the STAC ontology, we link common security concepts (e.g., `EncryptionAlgorithm`) to other existing security ontologies published online presented in the section 3.

A `Technology` is vulnerable to `Attack` (`hasVulnerability` property) and has specific `SecurityMechanism` (`isProtectedBy` property. An example, is that all wireless technologies have the `Jamming` attack in common due to the wireless communication, which is not the case for wired networks. We define a great deal of technologies and the related instances in the STAC knowledge base: `NetworkManagement`, `Web (ProgrammingLanguage, Ecommerce, Frameworks, Databases)`, wired (`Ethernet`) and wireless networks: `SensorNetwork`, `M2M`, `Wi-Fi`, `GSM (2G)`, `UMTS (3G)`, `LTE (4G)`, etc.

[5]http://lov.okfn.org/dataset/lov/
[6]http://datahub.io/fr/
[7]http://sindice.com/
[8]http://www.sensormeasurement.appspot.com/?p=rule
[9]http://validator.linkeddata.org/vapour
[10]http://graphite.ecs.soton.ac.uk/checker/
[11]http://oeg-lia3.dia.fi.upm.es/webOOPS/index-content.jsp
[12]http://linkeddata.org/

A Technology can be replaced by another technology more recent (isReplacedBy property). This is the case for cellular technologies: the GSM technology has been replaced by the GPRS technology.

We classify Attack according to the OSIModelLayer and the Technology. For example, the Jamming attack occurs in the PhysicalLayer and is specific to SensorNetwork whereas the SQLInjection occurs in the ApplicationLayer and is dedicated to Web applications.

We have referenced numerous technologies, attacks and security mechanisms according to the OSI model.

In the STAC ontology, we specify restrictions between attacks and the security mechanisms. For example, SensorAttack can exclusively be protected by SensorSecurityMechanism and WebAttack by WebSecurityMechanism: the VPN (Virtual Private Network) security mechanism is a web security mechanism and so cannot thwart sensor attacks.

The OSIModel concept is a collection of seven OSIModelLayer concepts which are {Physical, Link, Network, Transport, Session, Presentation, Application}Layer.

SecurityProperty is a concept that gives more information about security mechanisms. We describe thirteen security properties (e.g., Confidentiality, Authentication, Integrity, AccessControl, NonRepudiation), etc. to indicate that security mechanisms satisfy some of these security properties. For example, VPN satisfies the authentication, the confidentiality and the integrity properties.

SecurityMechanism is used to protect Application against specific Attack, they can be: (1) SecurityTool such as NetworkSecurityTool (Wireshark), WifiAttackTool (WepCrack), MessageEncryptionTool (PGP), Proxies, Sniffers (2) SecurityProtocol which are classified by technologies: WebSecurityProtocol (HTTPS) SensorSecurityProtocol (SPINS, TinySec, LLSP, MiniSec, ContiSec) WifiSecurityProtocol: (WPA2), and (3) CryptographicConcept: HashFunction (SHA), DigitalSignature (RSA), KeyManagement (IKE), AsymmetricAlgorithm (RSA, ECC) and SymmetricAlgorithm which are split into: BlockCipher (AES) and StreamCipher (RC4).

Numerous instances of security mechanisms are defined such as PGP, IDS, Firewall, Proxy, DMZ, ACL.

A SecurityMechanism can be itself composed of other security mechanisms. For example, the VPN security mechanism is composed of (dcterms:hasPart property) the IKE key management and the IPSec protocol which are both security mechanisms. Technologies are protected by specific security mechanisms. Indeed, sensor security mechanisms are devoted to secure the sensor technology, Wi-Fi security mechanisms protect Wi-Fi technologies, etc.

A SecurityMechanism can be replaced by another more secured (isReplacedBy property). An example is that in Wi-Fi technologies, the WEP security mechanism has been replaced by WPA1 which has been replaced by WPA2.

To help developers to choose the best security mechanism, there is a need to differentiate them by indicating their strengths and weaknesses. We design the concept called Feature to fulfill this need. The Feature concept is composed of several properties: Free, Flexible, Scalable, Secured, LowCostDeployment, LowEnergyConsuming, ExchangeKeyEasy and SuitableHeterogeneousCommunication. Hence, we can indicate that an AsymmetricAlgorithm is HighEnergyConsuming, but propose an easy solution to exchange keys (ExchangeKeyEasy). A SymmetricAlgorithm is LowEnergyConsuming, however, exchanging the keys is not an easy task. Another example is the difficult task to secure communications due to various protocols: there are three main security protocols to secure Wi-Fi communications: WEP, WPA1 and WPA2, the latter is the most secured security mechanism.

C. Prototype implementation

We present in this section the architecture and technologies used to implement both the STAC ontology/dataset and the STAC user interface. To demonstrate the feasibility of the proposed ontology, we develop the user interface in J2EE, use the Google Application Engine (GAE) and propose Web services REST (the Jersey implementation). The user interface is implemented with HTML5, CSS3, JavaScript and AJAX technologies. We used semantic web technologies to represent the STAC ontology and dataset: RDF, RDFS, and OWL. The STAC ontology has been referenced by the LOV (Linked Open Vocabularies) project. The Jena framework[13] is used to manage semantic data and the SPARQL language to perform the queries.

The ontology-based STAC application has been created to help the developers to design a secure IOT application. Developers look for information to secure their applications, using the user interface that we have developed. Our application, published online[14] proposes a menu composed of:

- STAC template. Users choose a specific technology and STAC displays all related attacks, security mechanisms, properties satisfied and features (Figure 3).
- The cryptography web page with encryption algorithms, hash functions, digital signatures, mode of operations and key managements (Figure 4).
- The security property web page and their methods.
- The attack and security mechanism interface containing threats, and their security mechanisms classified

[13] http://jena.apache.org/

[14] http://www.sensormeasurement.appspot.com/

Figure 3. STAC template

according the OSI model and the technologies (Figure 5).

- The sensor network web page that explains sensor protocols, sensor attacks, sensor security mechanisms and sensor key managements (Figure 6).
- The security for communication network web pages with GSM (2G), GPRS (2.5G), UMTS (3G), Wi-Fi, Bluetooth, Wimax, Machine-to-Machine (M2M) and Mesh networks.

In Figure 3, the developer chooses a technology (e.g., WiFi), all related attacks are display (e.g., Steal NIC) and the security mechanisms specific to the WiFi technology. Then, the developer chooses a security mechanism (e.g., WPA2) to obtain additional information: the security property satisfied (e.g., authentication) and the features (e.g., secured).

Figure 4 shows main cryptographic concepts. It explains that the encryption algorithm is either a symmetric or asymmetric, and the tooltip teaches that keys used in an asymmetric algorithm are different for encryption and decryption, allowing for easier key distribution. An instance of an asymmetric algorithm can be RSA. Symmetric algorithms can be either stream cipher (e.g., RC6) or block cipher (e.g., AES). The interface displays also hash functions (SHA), digital signatures (DSS), mode of operation (CBC) and key management (Diffie Hellman) by using a drop-down list.

The interface depicted in Figure 5 displays all attacks and proposes the security mechanisms to thwart them. For example, to thwart the eavesdropping attack, we propose the HTTPS security mechanism. A click on the drop-down list also proposes authentication method, directional antenna, encryption algorithm, and the VPN security mechanisms. We also indicate for security mechanisms the security properties satisfied and their features. The VPN satisfies the authentication, integrity, confidentiality, access control, privacy and authorization properties and features are low cost deployment and secured. In the OSI model section are classified all attacks and all security mechanisms according to the OSI model layer: the SQL injection occurs in the application layer, the PGP security mechanism protects the application layer, etc.

The interface as depicted in Figure 6 focuses on security

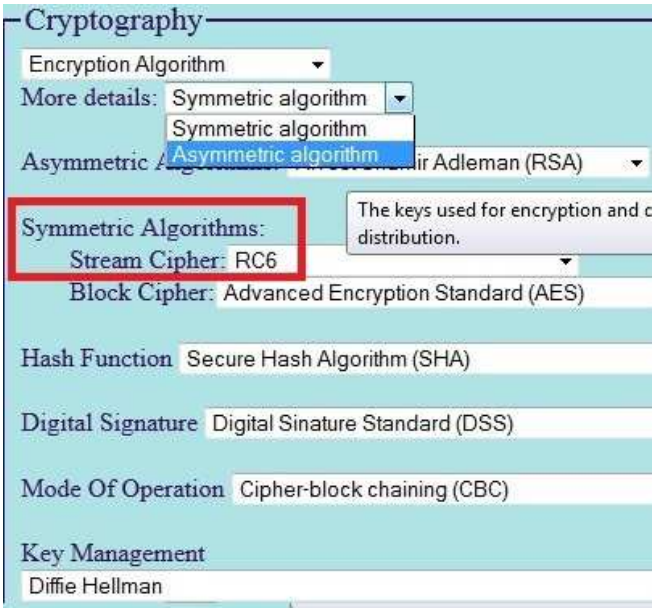

Figure 4. The cryptography interface

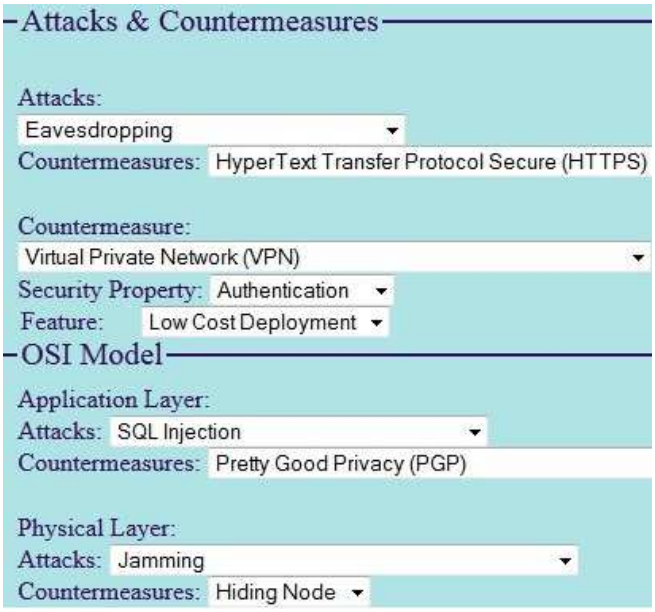

Figure 5. The attacks and security mechanisms interface

for sensor networks: sensor attacks and their security mechanisms. This interface indicates which security algorithms are used in sensor protocols (the SPINS sensor protocol is composed of (dcterms:hasPart property) the RC6 algorithm). The cryptography interface indicates that RC6 is a stream cipher algorithm which is a symmetric algorithm and so an encryption algorithm. With the help of the security property interface, we know that the encryption algorithm is a confidentiality method and satisfies the confidentiality property. We also indicate sensor key managements: the LEAP sensor

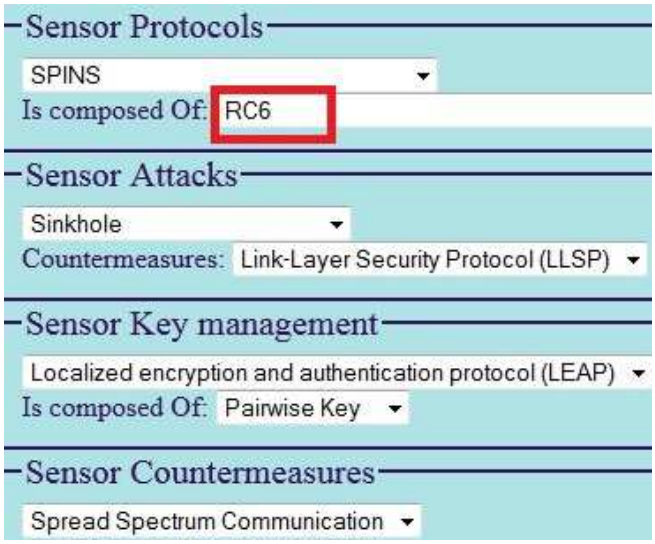

Figure 6. The sensor networks interface

key management is composed of (dcterms:hasPart property) four keys: pairwise key, cluster key, group key and individual key. A tooltip gives more information of all concepts: the definition of threats or security mechanisms. A click on each drop-down list shows all sensor protocols, sensor attacks, etc. The software developer who needs information about security in sensor networks goes directly to this interface.

D. Evaluation

At the beginning of this work, only 5 ontologies were published online and did not follow the semantic web guidelines. At the time of writing this paper, we have referenced 24 ontologies as following:

- 7 ontologies are not available yet. The authors do not reply to our email to publish online the ontology according to the semantic web best practices.
- 14 ontology are online, 10 do not follow the semantic guidelines yet, but 4 ontologies follow the semantic guidelines and are referenced by LOV.
- 1 ontology has been lost.
- 2 will be published online soon according to the authors.

The STAC ontology and dataset has been evaluated and accepted by the semantic web community since they are referenced by the LOV project. The STAC hub is linked to 4 security ontologies which respect the semantic web guidelines and are now referenced by LOV too thanks to our work. We validate the STAC knowledge base with semantic web tools such as RDF validator[15], RDF Triple-Checker[16] and fixing some errors with the Oops project[17] and Vapour[18]. The LOV project ask us to contribute to their project since we have explored the ontology-based security domain and other ones related to Internet of Things which were not referenced yet.

Further, we referenced all semantic bad practices and proposed the related guidelines in a draft document [10] for the oneM2M international standard for the technical semantic web part.

We sent a Google form[19] to fill to developers and researchers in computer science to test the STAC application: We obtained 28 responses[20] as following:

- 10 persons found the STAC application useful, 1 not, and 17 did not well understood the usability. We have to improve the user interface and the explanations.
- 20 were interested to know security related to wireless networks, WiFi 3G, 4G, Sensors. This is why we extended the STAC security knowledge base with new domains such as wireless networks, network management, mobile application, cloud e-commerce, web, etc.

SPARQL queries request the STAC knowledge base to return the needed information though the web services and the GUI.

V. Conclusion

In this article, we have presented a great deal of security ontologies to help software designers to choose security mechanisms to secure the ETSI M2M architecture, more precisely the IoT applications. We have been inspired by these ontologies to build an ontology-based security knowledge, called STAC, applied to numerous technologies and define the related attacks, security mechanisms, security properties, features, etc. The STAC ontology and dataset respect the semantic web best practices and are published online. The STAC application enables the developers to look for information to secure their sensor-based IOT application. As future work, we intent to automatically update this security knowledge base through a Google form, which will be automatically converted as instances in the STAC dataset. Another step will be to automatically integrate the security mechanism (e.g., AES using Java security API). Another future work will be to design a tool to automatically improve security ontologies according to the best practices.

Acknowledgment

The authors would like to thank the semantic web experts (Ghislain Atemezing, Raphael Troncy, Fabien Gandon, Bernard Vatant), Payam Barnaghi, Soumya Kanti Datta for their valuable feedback and colleagues/friends/students for fruitful discussions and help for the implementation. This

[15]http://www.w3.org/RDF/Validator/
[16]http://graphite.ecs.soton.ac.uk/checker/
[17]http://oeg-lia3.dia.fi.upm.es/oops/index-content.jsp
[18]http://validator.linkeddata.org/vapour

[19]https://docs.google.com/forms/d/1NKiMQPVR6X6Reioud0-WBZu1bmo3T1Ah7PZm9De-apk/viewform
[20]https://docs.google.com/forms/d/1NKiMQPVR6X6Reioud0-WBZu1bmo3T1Ah7PZm9De-apk/viewanalytics

work is supported by the Com4Innov Platform of Pole SCS[21].

REFERENCES

[1] Security ontology. http://semanticweb.org/wiki/File:OntologySecurity.owl.

[2] A. Alazeib and A. Diehl. An ontology for generic wireless authentication data. In *8th International Protege Conference-July*, pages 18–21, 2005.

[3] S. Beji and N. El Kadhi. Security ontology proposal for mobile applications. In *Mobile Data Management: Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on*, pages 580–587. IEEE, 2009.

[4] D. Boswarthick, O. Elloumi, and O. Hersent. *M2m communications: a systems approach*. Wiley, 2012.

[5] G. Denker, L. Kagal, T. Finin, M. Paolucci, and K. Sycara. Security for daml web services: Annotation and matchmaking. *The Semantic Web-ISWC 2003*, pages 335–350, 2003.

[6] G. Denker, S. Nguyen, and A. Ton. Owl-s semantics of security web services: A case study. *The Semantic Web: Research and Applications*, pages 240–253, 2004.

[7] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*, pages 1–10. IEEE, 2009.

[8] A. Evesti, R. Savola, E. Ovaska, and J. Kuusijärvi. The design, instantiation, and usage of information security measuring ontology. In *MOPAS 2011, The Second International Conference on Models and Ontology-based Design of Protocols, Architectures and Services*, pages 1–9, 2011.

[9] L. Frye, L. Cheng, and J. Heflin. An ontology-based system to identify complex network attacks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 6683–6688. IEEE, 2012.

[10] A. Gyrard and C. Bonnet. Semantic Web best practices: Semantic Web Guidelines for domain knowledge interoperability to build the Semantic Web of Things, 04 2014.

[11] A. Gyrard, C. Bonnet, and K. Boudaoud. The stac (security toolbox: attacks & countermeasures) ontology. In *Proceedings of the 22nd international conference on World Wide Web companion*, pages 165–166. International World Wide Web Conferences Steering Committee, 2013.

[12] A. Herzog, N. Shahmehri, and C. Duma. An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, 1(4):1–23, 2007.

[13] A. P. Joshi. *Linked Data for Software Security Concepts and Vulnerability Descriptions*. PhD thesis, University of Maryland, 2013.

[14] H. Kenfack, T. Ndié, E. Nataf, O. Festor, et al. Une ontologie pour la description des intrusions dans les rcsfs. In *CFIP 2011-Colloque Francophone sur l Ingénierie des Protocoles*, 2011.

[21] http://www.pole-scs.org/

[15] A. Kim, J. Luo, and M. Kang. Security ontology for annotating resources. *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*, pages 1483–1499, 2005.

[16] R. Lekhchine. *Construction d'une ontologie pour le domaine de la securite : application aux agents mobiles*. PhD thesis, University Mentouri, 2009.

[17] H. Neji and R. Bouallegue. Roadmap for establishing interoperability of heterogeneous cellular network technologies-1. *arXiv preprint arXiv:1207.3358*, 2012.

[18] H. Neji and R. Bouallegue. Roadmap for establishing interoperability of heterogeneous cellular network technologies-2. *Journal of Signal and Information Processing*, 3(3):402–411, 2012.

[19] H. Neji and R. Bouallegue. Roadmap for establishing interoperability of heterogeneous cellular network technologies-3. *International Journal of Computer Applications*, 54(5):17–27, 2012.

[20] N. F. Noy, D. L. McGuinness, et al. Ontology development 101: A guide to creating your first ontology, 2001.

[21] A. Razzaq, K. Latif, H. F. Ahmad, A. Hur, Z. Anwar, and P. C. Bloodsworth. Semantic security against web application attacks. *Information Sciences*, 254:19–38, 2014.

[22] A. Salahi and M. Ansarinia. Predicting network attacks using ontology-driven inference. *arXiv preprint arXiv:1304.0913*, 2013.

[23] A. Souag, C. Salinesi, and I. Comyn-Wattiau. Ontologies for security requirements: A literature survey and classification. In *Advanced Information Systems Engineering Workshops*, pages 61–69. Springer, 2012.

[24] B. Tsoumas, S. Dritsas, and D. Gritzalis. An ontology-based approach to information systems security management. *Computer Network Security*, pages 151–164, 2005.

[25] J. Undercoffer, A. Joshi, and J. Pinkston. Modeling computer attacks: An ontology for intrusion detection. In *Recent Advances in Intrusion Detection*, pages 113–135. Springer, 2003.

[26] P.-Y. Vandenbussche and B. Vatant. Metadata recommendations for linked open data vocabularies. *Version*, 1:2011–12, 2011.

[27] J. Vincent, C. Porquet, M. Borsali, and H. Leboulanger. Privacy protection for smartphones: an ontology-based firewall. In *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication*, pages 371–380. Springer, 2011.

[28] A. Vorobiev and N. Bekmamedova. An ontology-driven approach applied to information security. *Journal of Research and Practice in Information Technology*, 42(1):61, 2010.

[29] W. Znaidi, M. Minier, J. Babau, et al. An ontology for attacks in wireless sensor networks. 2008.